

Details of 50,000 Uber drivers breached

The Financial Times

By Sarah Mishkin

February 27, 2015

The personal information of about 50,000 Uber drivers has been accessed by an unknown third party, in one of the largest [data breaches](#) to hit the [\\$40bn company](#).

A Friday afternoon [announcement](#) from the ride-hailing app said it had discovered a bug in its systems last September that allowed unauthorised access to some drivers' names and license numbers. It fixed that bug, but a subsequent investigation revealed that there had been a "one-time unauthorised access" to the data last May.

Uber said it had not received any "reports of actual misuse" of the data and was notifying affected drivers, but security experts criticised its decision to wait months before alerting them to the breach.

"Five months is too long," said Tim Eades, chief executive of security firm vArmour.

Delays between a data breach being discovered and it being reported are common, he said. "They are a problem for consumers, who need to know to watch their credit reports and bills carefully to make sure their identities have not been stolen," said Chris Wysopal, co-founder of app security firm Veracode.

Uber's statement said it would provide affected drivers with one free year of identity theft protection monitoring.

Mr. Wysopal noted that the number of drivers affected was small compared to the tens of millions of names stolen in recent breaches at retailers and the health insurer [Anthem](#). That, he said, suggested that the intruder had only been able to access a limited portion of Uber's network.

"In those breaches when it's in the millions, it's that [the intruder] had free rein [of a corporate network] -- if they had that, they wouldn't have had just 50,000 names," Mr. Wysopal said.

Companies are governed by a patchwork of state laws requiring them to notify consumers about breaches, but can avoid notifying those affected if, for example, they are working with law enforcement or can argue that disclosure would impede an active investigation into the breach, say experts and lawyers.

“You can do a two-step around the disclosure guidelines as a corporation, but a lot of this comes back to your moral compass,” said Mr. Eades.

Uber said it had been investigating the scope and source of the breach since discovering the bug in September and had filed a lawsuit to help it collect more information on who had accessed its network.

It is not the first breach and privacy problem to hit the company.

Uber recently hired a prominent privacy lawyer to review its privacy practices and suggest areas for improvement. It took the step after reports surfaced that employees in its New York office had accessed the travel records of a journalist who covers the company and other employees had accessed at company events a so-called “God View” that showed all Uber rides in real time.

Earlier this month, Uber also apologised for leaving available online a record from a southern Californian office of items reported lost in Ubers. The database included dozens of passengers’ full names alongside the items they had lost, including many sets of car keys, iPhones, backpacks, and one pair of “cheap glasses, in a Prada box”.